



Unique Identification Authority of India  
Government of India

सत्यमेव जयते



# Unlocking face authentication

## Playbook



Knowledge Partner



# Table of contents

Acknowledgements.....	5
This playbook in a nutshell.....	7
<b>1. Journey of Aadhaar and authentication.....</b>	<b>11</b>
1.1. The evolution of <i>Aadhaar</i> in India .....	12
1.2. An overview of the authentication modalities.....	14
<b>2. Adoption of face authentication (FA) .....</b>	<b>19</b>
2.1. Face authentication and its adoption so far.....	20
2.1.1. Current use cases of face authentication.....	25
2.2. Integration and deployment of FA.....	30
2.2.1. Technical specifications for biometric authentication.....	30
2.2.2. Requirements to integrate FA.....	32
2.2.3. Integration using API calls.....	33
2.2.4. Demo workflow for face authentication.....	34
a) For testing in pre-production.....	34
b) For assisted transactions through FA.....	35
c) For self-use onboarding through FA.....	36
<b>3. Way forward for face authentication .....</b>	<b>37</b>
3.1. Potential use cases of face authentication.....	38
3.2. The UIDAI's efforts to enhance the adoption of face authentication .....	40
<b>4. Abbreviations.....</b>	<b>41</b>



# Acknowledgements



This playbook has been a collaborative endeavor of various individuals and institutions. On behalf of the Unique Identification Authority of India (UIDAI), we extend our sincere gratitude to all internal and external stakeholders who contributed to the development of this playbook on Face Authentication. This playbook represents a milestone in our ongoing efforts to enhance India's authentication and e-KYC ecosystem. We acknowledge the unwavering support from our colleagues, at the Technology Centre in Bangalore and the Head Quarters in Delhi, whose insights and perspectives significantly enriched the contents of this playbook.

We extend our gratitude to the *Aadhaar* authentication ecosystem participants including Authentication User Agencies (AUAs), KYC User Agencies (KUAs), Authentication Service Agencies (ASAs), and KYC Service Agencies (KSAs) who contributed to the discussions and deep-dives conducted with them. We are particularly grateful to the National Informatics Centre (NIC), Protean eGov Technologies, Tamil Nadu e-Governance Agency (TNeGA), Axis Bank, Airtel Payments Bank, India Post Payments Bank, PayNearby, and Reliance Industries Limited for their valuable input and participation in the development of this playbook.

We thank the MSC (MicroSave Consulting) team for their commendable work in gathering insights and co-authoring this playbook with UIDAI. Their support and dedication were instrumental in bringing this playbook to life. We also extend our appreciation to the Gates Foundation for their support.

We also want to thank our readers—your use of this playbook will keep the conversation going about the role of face authentication in India's *Aadhaar*-based authentication ecosystem.

## Who is this playbook for?



This playbook is a reference guide that will help introduce audiences to face authentication as a modality and provide an overview of its adoption along with prevalent use cases.

The playbook is for everyone, including requesting entities and end users, who want to learn more about *Aadhaar* face authentication and integrate it with their applications.





# This playbook in a nutshell



*Aadhaar*, India's unique identification system, has evolved significantly since its inception in 2009. It has become a cornerstone for identity verification and service delivery. Over the past decade, *Aadhaar* has transformed into a critical infrastructure for social welfare programs, financial inclusion, and digital governance. Today, it significantly impacts the lives of more than 1.4 billion people, with nearly every adult in the country now having access to *Aadhaar* as a formal ID. *Aadhaar*'s strength lies in its use of biometric authentication to verify and authenticate individuals using modalities, such as fingerprint, iris, and, more recently, facial authentication. These modalities have helped ensure the uniqueness of each identity, prevent duplication, and reduce fraud in government programmes.

The Unique Identity Authority of India (UIDAI) introduced fingerprint authentication as the first biometric modality. Its widespread use can be attributed to its relative simplicity, cost-effectiveness, and the wide availability of fingerprint-scanning devices. It has proven accurate, with an 81% success rate. Fingerprint authentication has also ensured that subsidies and benefits reach the intended recipients through fingerprints as the identifier and eased the eKYC process during customer onboarding across the financial and telecom sectors. However, the number of attempts required to authenticate may be higher in some cases due to environmental factors, such as dust, or moisture, wear and tear, manual labour, old age, etc. The UIDAI then introduced iris as a supplementary modality for authentication. Iris-based authentication also offers high accuracy (81%) and does not degrade with age or environmental factors, which makes it particularly useful for individuals whose fingerprints are not captured easily. However, iris recognition devices require a certain level of proficiency for proper handling and storage.

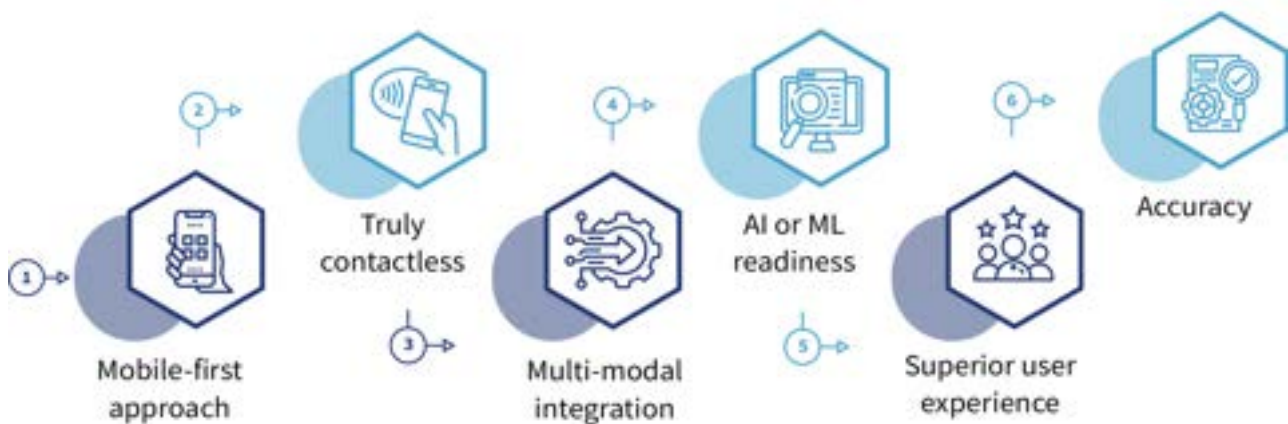
In 2018, the UIDAI introduced face authentication as an additional layer of authentication, which further expanded *Aadhaar*'s inclusivity and accuracy and provided a contactless alternative for biometric authentication. Face authentication is particularly beneficial for the elderly, people with disabilities, and others who may face difficulties with fingerprint or iris scans. It provides the highest levels of accuracy at 84%, compared to both fingerprint and iris, and only requires the use of cameras on smartphones, which makes it more accessible and user-friendly.

More than 55 million transactions are conducted each month using face authentication across 56 onboarded banking and non-banking authentication user agencies (AUAs). Moreover, face authentication transactions grew significantly by 649% over the past year. Some financial institutions



now use face authentication to streamline KYC processes, which has sped up customer onboarding and enhanced the overall customer experience. Today, face authentication's growing adoption extends beyond financial services to benefit government services, travel, security, and other sectors. Currently, people use face authentication in the assisted mode to complete a full KYC and in the self-use mode to mark attendance. Some banks have now started to pilot a completely remote KYC process through face authentication and video KYC.

Face authentication continues to improve access to service delivery for unserved and underserved people, thanks to features, such as its mobile-first approach, superior customer experience, contactless nature, multi-modal integration, artificial intelligence and machine learning readiness, and high accuracy.



Face authentication has significant potential for widespread adoption in India, especially given the rapid increase in smartphone penetration and advancements in AI and ML technologies. As more Indians gain access to smartphones with high-quality cameras, face authentication can become more prevalent and offer a seamless and convenient mode to verify identity. This modality also reduces the need for specialized hardware, such as fingerprint or iris scanners, to lower the overall cost of implementing biometric authentication at the population scale.

Face authentication can potentially diversify across sectors such as the banking and payments industry by enabling fully digital bank account opening, streamlining onboarding and enhancing customer convenience. It can also strengthen fraud management by integrating AI and multi-factor authentication, ensuring security for high-value transactions. It can also streamline the good governance use cases by easing the process for beneficiary identification and enhancing service delivery in other government programmes. Face authentication can also address current challenges and improve the success rate while authenticating AePS transactions. Additionally, face authentication can be a part of a risk-based approach to authentication by incorporating adaptive authentication. This system assesses the risk of the transaction and accordingly adjusts the authentication modality or modalities to be used.

However, concerns over issues, such as lighting conditions and compatibility with certain Android-based smartphones, need to be considered to drive the adoption of face authentication further. AUAs and sub-AUAs may also face risks like cyber fraud and deepfakes with face authentication. However, UIDAI's advanced algorithms and liveness detection strengthen security by analyzing facial contours and adding unpredictable prompts. The UIDAI continues to invest to improve

the technology's accuracy and reliability to ensure it can be used alongside other modalities for robust and secure authentication, while continually refining these safeguards and collaborating with industry stakeholders to enhance security, accessibility, and integration.

Apart from a snapshot of the current status of the adoption of face authentication, the playbook has also incorporated some workflows to illustrate potential ways to integrate face authentication for interested AUAs and KUAs. To complete face authentication, entities or users need to fulfil certain specifications such as a device with an embedded camera, such as a smartphone. They also need to download and run a headless app, FaceRD. The AUA application in the smartphone invokes the FaceRD application to capture, process, and package the face image details. This data is shared with the AUA application and sent to the UIDAI's Central Identities Data Repository (CIDR) for a 1:1 match.

This playbook will help anyone who wants to learn more about face authentication and practitioners who engage closely with the authentication ecosystem or operate in it. These could be public or private entities that currently verify and authenticate the identities of individuals across different sectors, such as banking, technology, and telecom, among others. The playbook also has important information for both business and management personnel as well as the technology leads and teams.



“ Be yourself; everyone else is already taken ”

- Oscar Wilde





# 1

## Tracing the journey of *Aadhaar* and authentication in India



## 1.1. The evolution of *Aadhaar* in India

*Aadhaar*'s journey in India is an incredible story of how technology can drive social change. What started in 2009 as a project by the Unique Identification Authority of India (UIDAI) to give every resident a unique ID has now become a key part of the country's digital infrastructure.

- *Aadhaar* is the world's largest biometric digital identity program, with a whopping 97%<sup>1</sup> of India's population enrolled as of August 2024,
- Nearly every adult in the country now has *Aadhaar* as a formal ID, and
- *Aadhaar* has also saved the government a massive INR 3,485 billion<sup>2</sup> (about USD 41.52 billion) in subsidies and transfers since 2013 by cutting out 100 million fake beneficiaries.

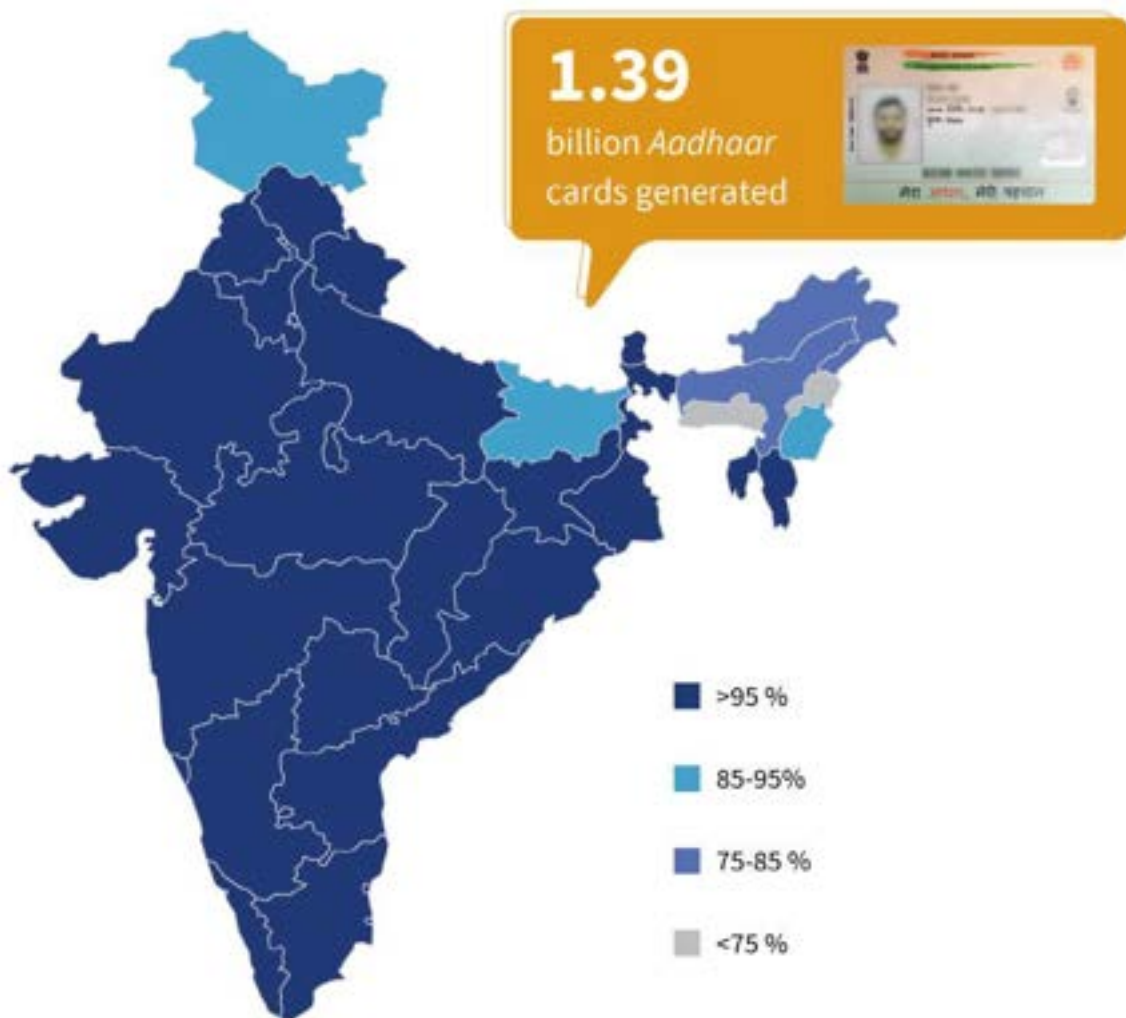


Figure 1: Status of *Aadhaar* penetration in India

Before *Aadhaar*, people in India verified personal identities manually and with paper documents, which made the process slow, costly, and vulnerable to fraud. Different agencies issued multiple paper IDs, which forced governments, banks, and other institutions to rely on documents that were difficult to verify and easy to forge.

UIDAI introduced *Aadhaar*-based authentication to tackle these challenges by offering a digital, online identity platform. Now, *Aadhaar* number holders can instantly validate their identity anytime, anywhere. This system uses two key processes: Authentication and verification.

- Authentication confirms if the person is who they claim to be; the identity is ascertained by matching their biometrics information against the *Aadhaar* database; and
- Verification checks the accuracy of the *Aadhaar* information without referring to real-time online authentication and verifies only by offline means.

As per the *Aadhaar* (Authentication and Offline Verification) Regulations, 2021, *Aadhaar* authentication is the process by which the *Aadhaar* number, along with the demographic information, such as name, date of birth, gender, or biometric information of an *Aadhaar* number holder, is submitted to the Central Identities Data Repository (CIDR) for verification. The CIDR is a centralised database that stores all *Aadhaar* numbers and corresponding demographic and biometric data. It verifies the correctness of this data based on the information available in the database.



*Aadhaar* authentication can be done in two ways: 1) Yes or No, which generates only a “Yes/No” response from UIDAI and helps identify a person’s identity claim through the response, and 2) electronic Know Your Customer (e-KYC), which generates a response containing a photograph and demographic details of the *Aadhaar* number holder upon a successful *Aadhaar* authentication. Offline verification is the use of *Aadhaar* for identity verification and KYC locally, without sending data to and receiving response from UIDAI online. The resident directly provides digitally signed *Aadhaar* information in QR or XML format to the organization instead of the organization receiving it from UIDAI.

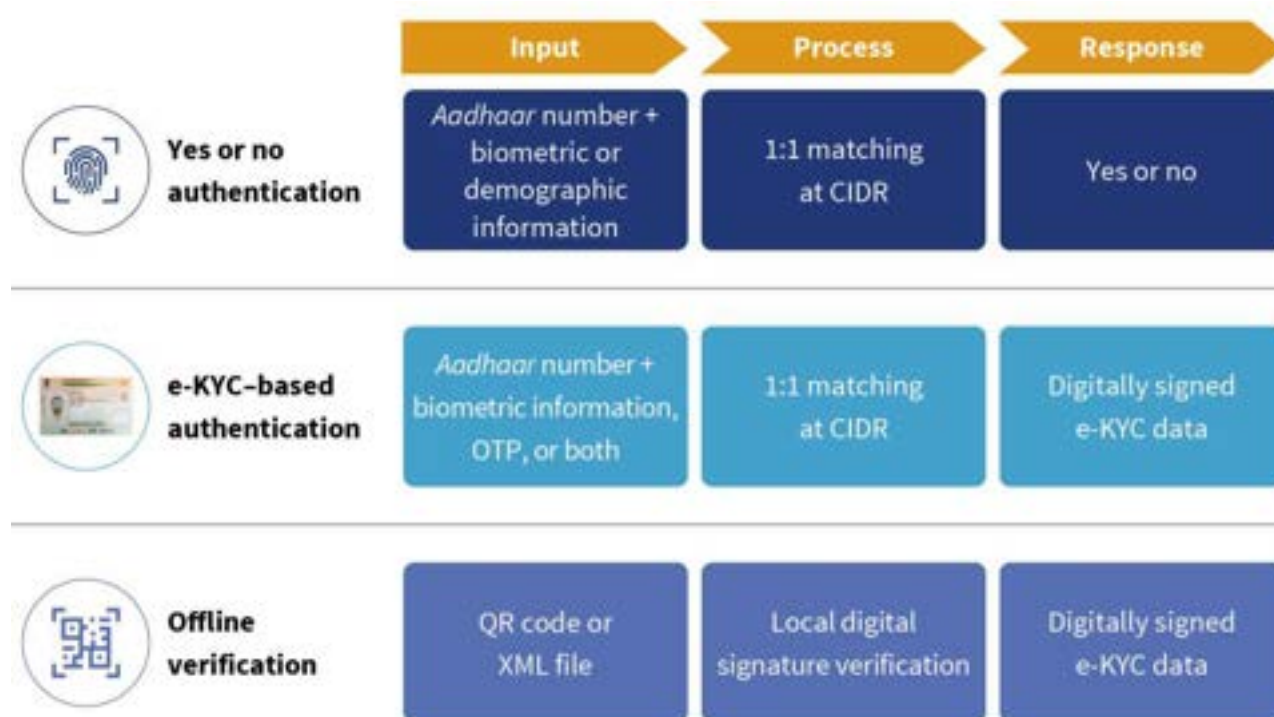


Figure 2: A snapshot of the authentication and verification methods in India

Over the years, *Aadhaar* authentication has witnessed exponential growth, with the annual authentication transactions growing at a CAGR of 150%, from 2.4 million transactions in FY 2012-13 to 22 billion annual transactions in 2023-24. The authentication and e-KYC transactions also grew sharply to 130 billion and 20.5 billion, respectively<sup>3</sup>.



Figure 3: Growth in *Aadhaar* authentication transactions

## 1.2. An overview of the authentication modalities

In 2011, UIDAI rolled out fingerprint authentication, which quickly became the go-to option for many people across India because of its simplicity. Whether it is the yes/no authentication or e-KYC, fingerprint authentication is now widely used in sectors, such as banking, telecom, property transactions, e-sign services, and social protection programs like direct benefit transfers. *Aadhaar*-based authentication, especially with fingerprints, has made financial transactions easier and more accessible, particularly through the *Aadhaar* Enabled Payment System (AePS). However, people who do hard manual labour or are older sometimes struggle with fingerprint authentication because their fingerprints may have deteriorated over time. There have been instances of security risks in financial transactions, which include spoofing through cloned fingerprints, such as those made from silicon replicas. Fingerprint-based authentication continues to be the most used modality, with an average of approximately 1,500 million<sup>4</sup> monthly transactions (see Figure 4). The growth in the transactions continues to remain broadly consistent.

In 2013, the UIDAI rolled out iris-based authentication to tackle the problem of fading fingerprints, especially among vulnerable groups, and to make *Aadhaar*-based authentication more accurate and efficient. Iris scanning offered a touch-free alternative and became essential for the distribution of cash benefits during the COVID-19 pandemic. The government installed 250,000<sup>5</sup> iris devices in



Public Distribution Systems (PDS), pension distribution, and beneficiary authentication for various government programmes.

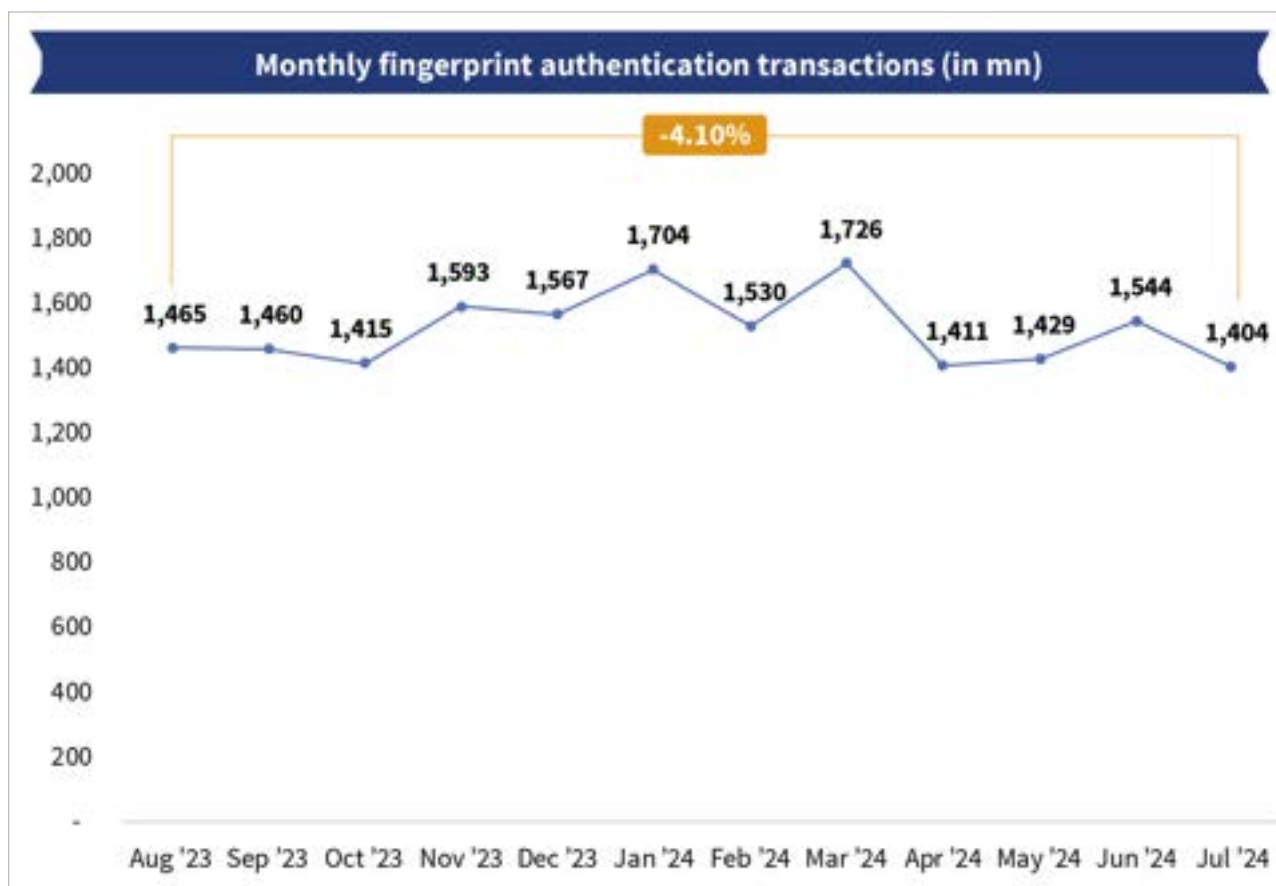


Figure 4: Monthly adoption of fingerprint authentication modality

#### **Fingerprint Image Record (FIR) - Fingerprint Minutia Record (FMR)**

**implementation in single PID block (Personal Identity Block):** To make *Aadhaar* authentication more secure and to enhance the liveness properties of fingerprint authentication, UIDAI has introduced the feature of FIR-FMR in a single PID block. The major focus of implementing the single PID block concept is to eliminate the fraudulent activities in various banks, financial entities, AePS, and other *Aadhaar* applications for residents and to make fingerprint-based authentication more secure and liveness detection efficient. All fingerprint authentication transactions are performed in FMR-FIR single PID capture modality.



Several banks also experimented with iris as an option for authenticating AePS transactions, where iris scanning authenticated most users in a single attempt to improve their overall transaction experience. The data in Figure 5 also shows a growth of approximately 90%<sup>6</sup> for iris transactions from August 2023 to July 2024. However, a few concerns remain around the usage of iris authentication. These concerns include the high cost of the device, which is approximately ₹ 3,500 (USD 36) compared to ₹ 2,000 (USD 24) for fingerprint scanners, and the complexity of operating the device compared to fingerprint scanners.

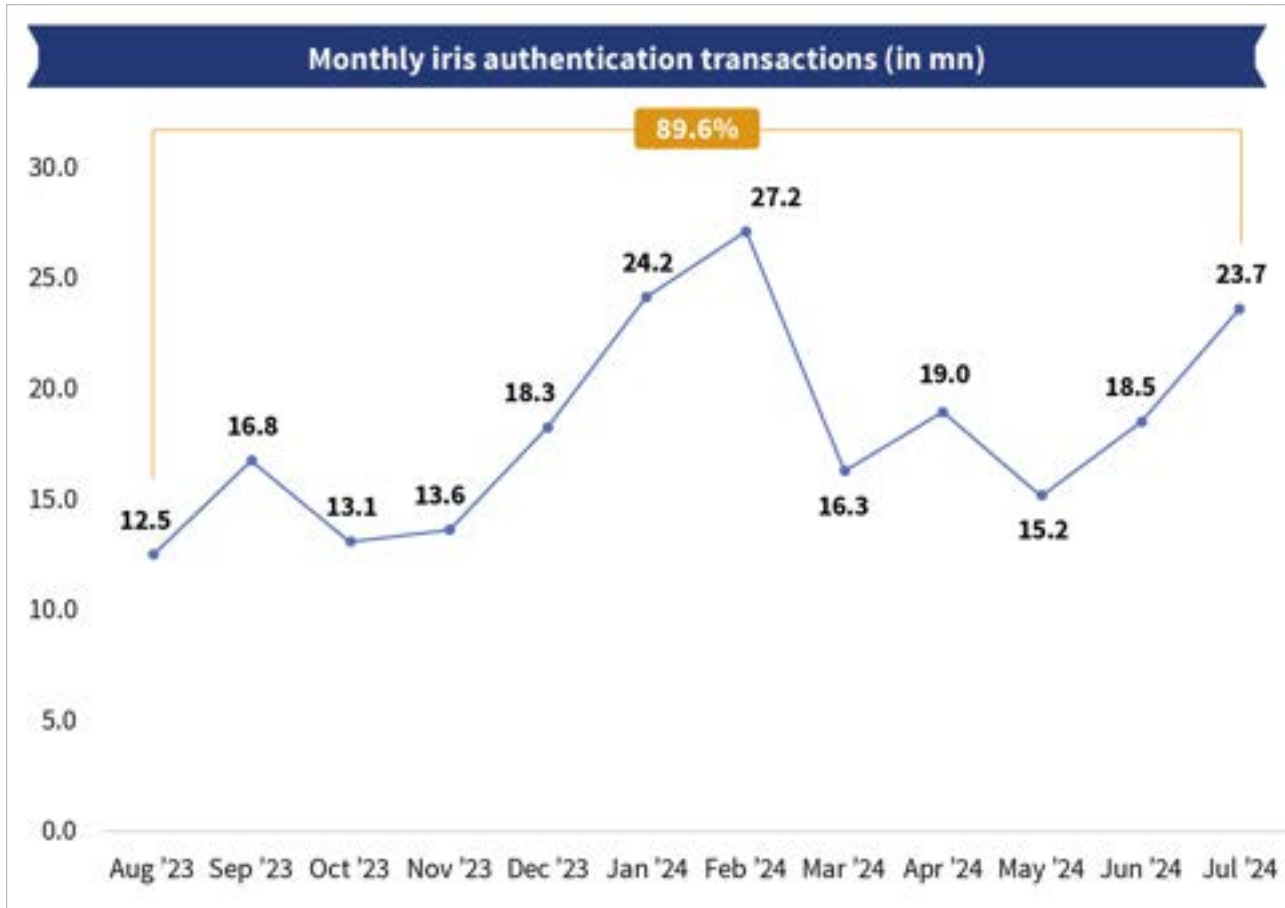


Figure 5: Monthly adoption of iris authentication modality

The rapid pace of technological innovation, the rise in smartphone penetration, and the availability of good quality smartphones with cameras at affordable cost in the country mandates that customer privacy and protection measures remain paramount. This has also resulted in traditional biometric authentication methods like fingerprint and iris authentication giving way to more sophisticated systems that include face match and liveness detection.

In 2021, UIDAI launched face authentication as a mode to further improve the accuracy, reliability, and security of *Aadhaar*-based authentication modes and offer a contactless way of authenticating users. Moreover, face authentication is also a viable mode of authentication for physically and visually disabled individuals and geriatric people needing assistance in the authentication process.



The infographic below highlights some major milestones in the evolving journey of *Aadhaar* and its authentication in India, which have helped improve user experience and service delivery across different sectors and stakeholders in the ecosystem.

### 2009- 2010 - The Aadhaar project's launch

- The UIDAI launched the Aadhaar project to provide every Indian resident with unique identification numbers.
- Fingerprint authentication was chosen as the primary modality due to its relatively low cost and ease of use.



### 2011-2012 - The introduction of fingerprint authentication

The formal launch of fingerprint authentication led to *Aadhaar*'s integration with the delivery of services for various government-led initiatives. These included initiatives for food support, employment support, and biometric attendance systems (BAS), among others.



### 2013 - Introduction of iris authentication, OTP, and e-KYC services

- The UIDAI launched iris, OTP-based authentication as an alternative mode to fingerprint authentication.
- e-KYC services introduced to transform the KYC services into a more secure and paperless process.
- Launch of Jeevan Pramaan- Digital Life Certificate for pensioners.



### 2016 - Legislative and regulatory foundations

- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016, provided the legal framework for Aadhaar, which included its use for the delivery of subsidies and services.
- The Aadhaar (Authentication) Regulations, 2016, detailed the processes and standards for Aadhaar authentication, which included data security and privacy measures.



### 2017 - 2018 - The UIDAI's guidelines and the RBI's measures for financial inclusion

- The UIDAI issued landmark guidelines that significantly shaped Aadhaar's technical and operational landscape. The e-KYC process guidelines ensured that all organizations used Aadhaar for verification in a standardized and secure manner. Biometric authentication standards were set for fingerprint, iris, and, later, face recognition, which ensured high accuracy across different methods.
- The RBI's endorsement of the JAM (Jan Dhan-Aadhaar-Mobile) trinity signalled the integration of zero-balance bank accounts, Aadhaar, and mobile numbers to create a powerful platform for direct benefit transfers.
- Specific guidelines were issued for Aadhaar e-KYC's usage in banking to simplify the account opening process.





**2019 - Aadhaar paperless offline e-KYC**

- Offline e-KYC services were launched to tackle challenges, such as lack of a reliable Internet connection, and to enhance the privacy and security in the KYC process.

**2020 - Policy refinements and technological upgrades**

- The Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020, allows Aadhaar authentication for purposes such as good governance, prevention of leakage of public funds, and the promotion of ease of living.
- Artificial intelligence (AI) or machine learning (ML) technologies were integrated to enhance *Aadhaar* authentication's security and accuracy.

**2021 - Launch of face authentication**

- Face authentication services were extended to all authentication user agencies (AUA) or KYC user agencies (KUAs) in the ecosystem.
- Services, such as Jeevan Pramaan, introduced face authentication to help pensioners generate digital life certificates easily.

**2022 - Enhancement of the security of Aadhaar authentication and widening UPI's use**

- The UIDAI announced the upgrade of existing L0 fingerprint authentication devices to L1-compliant devices to improve fingerprint authentication's overall security and accuracy.
- UPI's integration with *Aadhaar* sought to foster financial inclusion through the expansion of its potential user base. The integration sought to spread UPI services to non-debit card holders.

**2023 - Growing adoption of face authentication**

- Face authentication transaction numbers grew at a staggering ~50 million transactions monthly.

**2024 - Launch of face authentication for IOS**

- UIDAI extended the use of the FaceRD application to IOS devices, in addition to Android



Figure 6: Timeline of major milestones in the journey of *Aadhaar* and its authentication in India



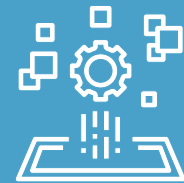
# 2

## The rise in the adoption of face authentication



Today’s technologies, from cameras to self-driving cars, heavily rely on computer vision, a branch of artificial intelligence (AI) that interprets visual data. By using machine learning and neural networks, computer vision enables systems to extract valuable insights from digital images, videos, and other visual inputs. This ability to ‘see’ and understand visual information has revolutionised various industries, including business, entertainment, transportation, healthcare, and daily life. The surge in visual data from devices, such as smartphones, security systems, and traffic cameras has significantly driven the growth of computer vision applications.

A prominent example is face authentication, which uses advanced algorithms to analyse facial features and verify identity using artificial intelligence (AI) and machine learning (ML) based solutions. The precision of these systems is closely linked to the sophistication of the underlying computer vision technology, which makes them crucial for secure digital interactions and improved user experiences.



## 2.1. Face authentication and its adoption so far

**Face authentication** is a 1:1 matching process in which an individual’s live facial image is compared to their pre-registered image in the *Aadhaar* database, and explicit consent is required for the process. This differs from face recognition, which is a 1: N (one-to-many) matching process that involves comparing multiple images in a database.

As biometrics evolve, face authentication is becoming increasingly important for identity verification due to its convenience, security, and adaptability, which has increased its relevance across various applications in today’s digital world.

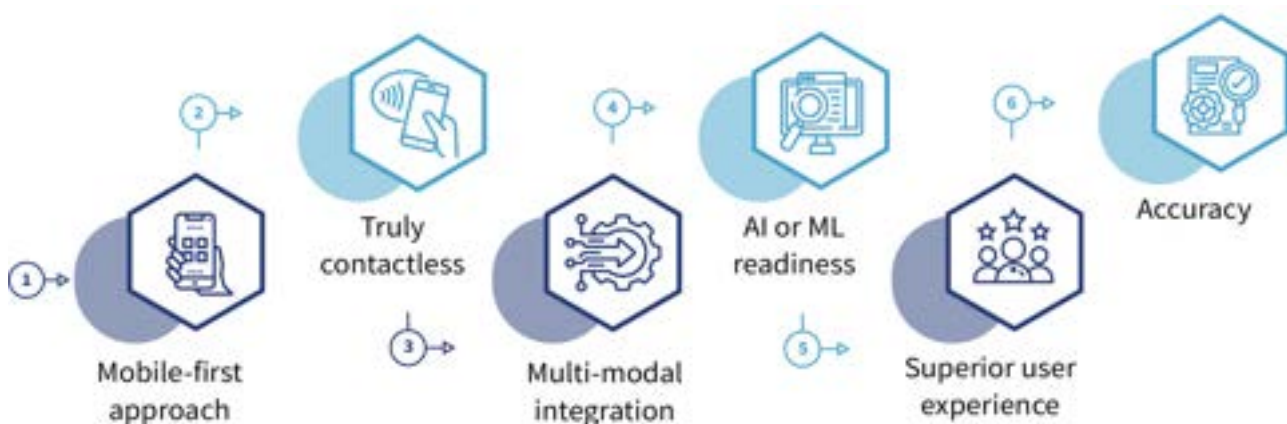


Figure 7: Key features of face authentication

**Mobile-first approach:** Face authentication has been widely adopted due to its seamless integration with mobile devices, Android and iOS. In a world where smartphones and tablets are extensions of ourselves, this technology allows users to unlock devices, authorise payments, and access secure apps with a glance, which makes it highly accessible to millions.

**Truly contactless:** After the COVID-19 pandemic, the contactless nature of face authentication offers a significant advantage. Unlike fingerprint scanners or physical tokens, face authentication technology requires no physical touch, which makes it both hygienic and convenient. Users simply look at their devices for the system to verify their identity, which enhances user experience and reduces device wear and tear.

**Multi-modal integration:** Face authentication's flexibility allows it to combine with other biometric methods, such as fingerprints, iris authentication, or OTPs, to create a multi-layered security approach. This versatility makes it a robust solution for diverse environments.

**AI/ML readiness:** Face authentication's effectiveness is driven by its integration with AI and machine learning, which enables continuous iteration and improvement. These technologies enhance the system's ability to recognise faces accurately in various conditions, adapt to new challenges, and ensure it remains future-proof.

**Superior user experience:** Face authentication offers a superior user experience with its speed, ease of use, and reliability. The process is near-instantaneous and requires only a glance to unlock devices or authorise transactions.

**Accuracy:** Internal metrics indicate face authentication transactions have an 84%<sup>7</sup> success rate, and this number is likely to improve as the UIDAI enhances its core machine learning models.



All these factors have been sparking more interest from stakeholders who want to explore and integrate face authentication into different use cases across various sectors.

Since its introduction, face authentication has seen significant adoption, with more than 55 million monthly transactions as of July 2024 across the 56 onboarded banking and non-banking authentication user agencies (AUAs). The graph highlights the growing adoption of face authentication by banks and other entities with a compounded annual growth rate of 649% over one year from Aug '23 to Jul '24.

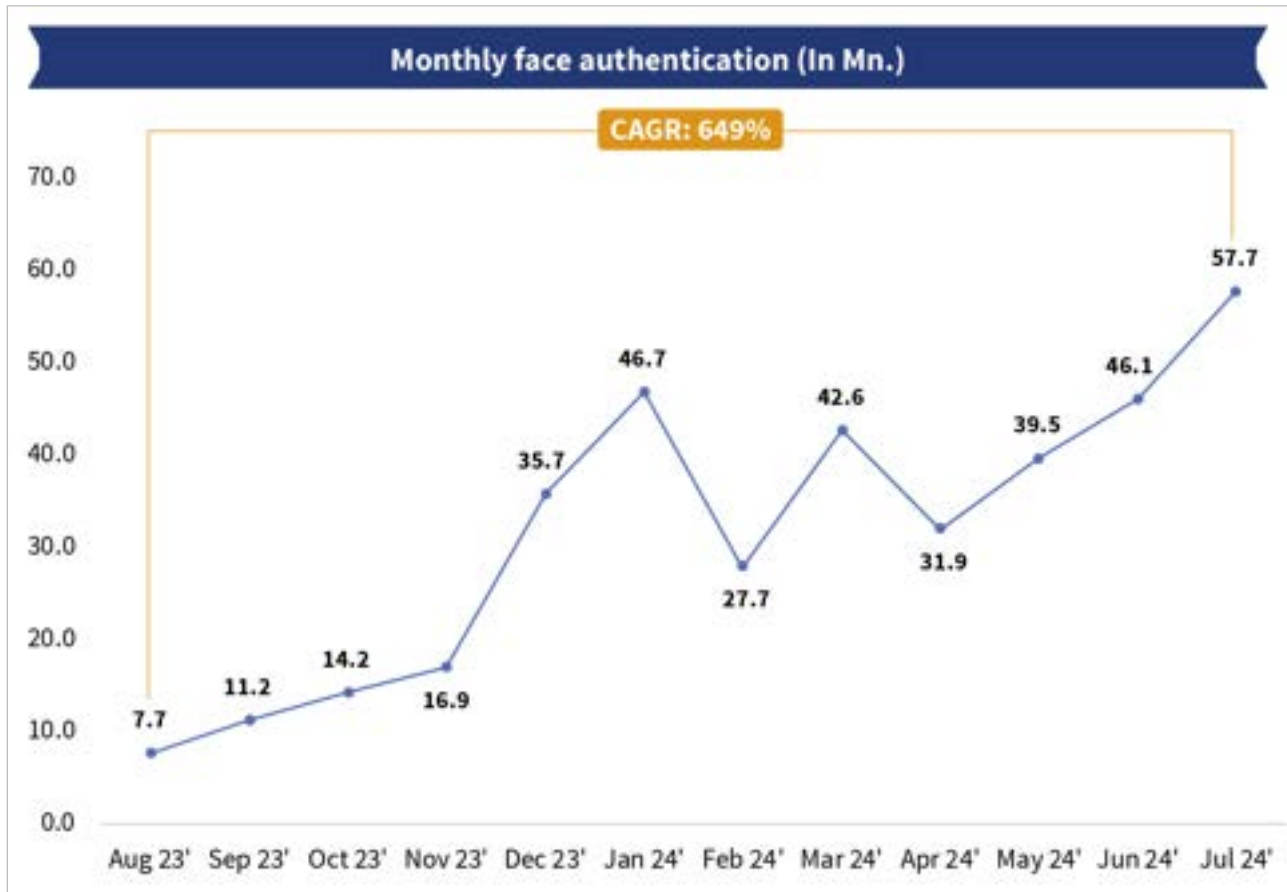



Figure 8: Growing adoption of face authentication

While face authentication offers both assisted and self-use modes, eKYC transactions are presently being conducted in the assisted mode. Several entities are in the process of pilot-testing the self-use mode as well.


**Assisted mode**

In the assisted mode, authentication needs to be completed on the financial service provider employee's device. For example, a postman/ BC agent supporting the opening of a bank account.










**Self-use mode**

In the self-use mode, face authentication is part of the video KYC process that can be completed from any location by the customer. For example, account opening through a bank application.










While face authentication offers several advantages over fingerprint and iris-based modes, a few potential areas need consideration and improvement. A quick comparison of the user experience, enablers, and considerations and challenges across the three modalities are as follows:

Parameter 	Fingerprint 	Iris 	Face 
 <p><b>Success rate*</b></p>	<b>81%</b>	<b>81%</b>	<b>84%</b>
 <p><b>User experience</b></p>	This mode is generally quick and easy to use and is considered to be the easiest modality for the user to understand.	The device needs to be positioned close to the eyes correctly to authenticate.	Face authentication provides a contactless and convenient authentication experience.
 <p><b>Enablers to adoption</b></p>	<ul style="list-style-type: none"> <li>Fingerprint is a widely popular modality due to its long-standing existence, ease of use, and familiarity among users.</li> <li>It is a cheaper authentication modality compared to iris devices, as fingerprint scanners cost around INR 2,000.</li> <li>Fingerprint scanners are compatible with almost all smartphones.</li> </ul>	<ul style="list-style-type: none"> <li>Iris authentication also offers a high success rate with fewer attempts to authenticate compared to fingerprint, as stated in the UIDAI PoC testing, as it is not affected by any external environmental conditions.</li> <li>Iris authentication is faster than fingerprint authentication and requires only a single attempt to authenticate in most cases.</li> <li>This mode offers high-security levels, as iris data is difficult to spoof.</li> </ul>	<ul style="list-style-type: none"> <li>Face authentication is useful for users who have worn off fingerprints or have physical disabilities.</li> <li>It is the cheapest authentication modality, as it does not require an additional device for authentication (assuming the user already has a compatible smartphone with an internet connection).</li> <li>Face authentication is easier to deploy in sensitive environmental conditions, such as in dusty weather and rains, as it only requires a smartphone camera.</li> </ul>

\* Success rate highlights the percentage of successful transactions among all transactions in a given period. This could include multiple attempts by the same person, and does not imply any denial of service.

Parameter 	Fingerprint 	Iris 	Face 
		<ul style="list-style-type: none"> <li>Iris devices provide contactless authentication, which makes them safe and secure and increases the device's life.</li> </ul>	<ul style="list-style-type: none"> <li>Face authentication is highly scalable for different stakeholders as it uses existing smartphone cameras and reduces the need for additional hardware.</li> <li>It provides higher security due to the liveness detection algorithm that prevents spoofing with photographs.</li> </ul>
 <p><b>Considerations and challenges</b></p>	<ul style="list-style-type: none"> <li>The fingerprint modality is susceptible to fraud or spoofing due to cloning or replication of fingerprints.</li> <li>The number of attempts required to authenticate may be higher in some cases due to environmental factors, such as dust, moisture or skin conditions, wear and tear, manual labour, old age, etc.</li> <li>Fingerprint authentication is costlier than face authentication due to the device's cost and reduced longevity due to regular contact and wear and tear.</li> </ul>	<ul style="list-style-type: none"> <li>Iris authentication requires specialised iris scanners, which have to be procured only from empanelled vendors.</li> <li>These scanners are expensive (~INR 3,500) compared to those used in other modalities.</li> <li>Iris authentication involves a steep learning curve to start using the device, which impacts its scale-up potential.</li> <li>It requires a stable position of the device and the user and could be uncomfortable for some users.</li> </ul>	<ul style="list-style-type: none"> <li>Face authentication can be affected by environmental conditions, such as low lighting.</li> <li>Some models of smartphones, which are not type-tested, may face a challenge when using face authentication.</li> <li>Devices that do not support Google or the IOS mobile app security cannot use face authentication.</li> </ul>

### 2.1.1. Current use cases of face authentication

Face authentication is becoming more important across various sectors in India because it offers better security and convenience. For example, some financial institutions have started to use it to simplify KYC processes, which has made it easier and faster for them to onboard customers and improved the overall experience in the process.

The growing adoption of face authentication means many entities use it for non-financial services as well across sectors, such as government services, travel, and security, among others. A snapshot of the existing use cases of face authentication is highlighted below:



Figure 9: Snapshot of existing face authentication use cases





### India Post Payments Bank (IPPB): Cutting down authentication turn-around-time (TAT) and improving customer convenience

Currently, IPPB uses face authentication to generate digital life certificates (DLCs). It is in the final stages of integrating face authentication into AePS transactions and other use cases, such as Re-KYC and account opening.

At present, IPPB can open ~80,000 new bank accounts through *Aadhaar* authentication and process ~40,000 AePS transactions daily. IPPB intends to equip its vast network of end-users with face authentication-compatible smartphones and use this network.

Face authentication would provide IPPB with convenience, user-friendliness, speed, and an easier training process for its end-users. Postal workers must only follow the steps on the screen when they use face authentication. This saves them several minutes that are usually needed to set up the fingerprint device, attach it, and wait for it to configure.



## b) Non-financial use cases of face authentication

### Telecom

Almost all telecom companies have adopted face authentication to onboard customers. While fingerprint continues to be the predominant mode of authentication, the Department of Telecommunications (DoT) defined the process to use face authentication for eKYC in 2023. Industry stakeholders indicate that the use of face authentication has eliminated device dependency and maintenance. It is faster, simpler to operate, and more reliable than other modes.

### Telecom (Reliance Jio): Simplified, quick, and convenient customer onboarding through face authentication

Jio rolled out the face authentication feature in August 2023 to conduct e-KYC transactions. Until then, fingerprint-based authentication was the primary modality for Jio's e-KYC process. Fingerprint authentication required the management of the supply chain, support, updates, and compliance for those many fingerprint devices, as Jio had more than 200,000 retail partners countrywide. Face authentication presented a new, more robust, and cost-effective modality to conduct e-KYC. It also made the process quicker and more convenient compared to fingerprint authentication, which enhanced customer experience.

Transactions through face authentication grew from 20% of total transactions in January 2024 to 41% in April 2024 of total Jio's e-KYC. Moreover, face authentication has showcased an average success rate of 84-86% from August 2023 to April 2024.





### National Informatics Centre (PDS): Ensuring easy last-mile authentication

The NIC plays a pivotal role in *Aadhaar* authentication's implementation and support across various government services and initiatives. NIC has integrated *Aadhaar* authentication into the public distribution system (PDS) to ensure accurate beneficiary identification and reduce fraud.

PDS conducts more than 1 million authentication transactions daily across different geographies in India. Although fingerprint remains the first method of authentication, PDS has started to use face authentication for exception handling. Face authentication has become an effective modality for PDS for different use cases, such as home delivery of benefits to some vulnerable sections of the population. This allows the dealers and officers to simply carry a smartphone to conduct a quick authentication and deliver the ration to the beneficiaries' homes.



## Good governance

Face authentication has also been used for other use cases, such as the *Aadhaar* Enabled Biometric Attendance System (AeBAS), which seeks to bring accuracy and transparency to the attendance system at government offices by ensuring accurate and real-time tracking and an instant data record. The system has conducted more than 1.2 million<sup>19</sup> authentication transactions as of August 2024.

Good governance use cases also include the following:

- **Telangana State Technology Service:** Registration and Stamp duty collection; attendance management

### AeBAS: The facilitation of improved attendance marking and monitoring through face authentication

The *Aadhaar* Enabled Biometric Attendance System (AeBAS) is a digital attendance system used primarily in government offices and institutions to mark employee attendance through *Aadhaar*-based biometric authentication.

During FaceRD's development phase, the NIC helped test, create a sample app, and provide feedback. Initially, touchless face authentication was developed for fixed terminals. However, mobile-based clients were developed for AeBAS with the growing need for mobile solutions. Users could also mark their attendance on their smartphones with the FaceRD application.

AeBAS provides facilities for geo-fencing based on the user's GPS coordinates and location control based on the official requirements.





- Generation of digital life certificates for pensioners under the *Jeevan Pramaan* programme

### **Jeevan Pramaan (DLC generation): The enhancement of customer convenience through reduced turn-around-time for DLC generation**

*Jeevan Pramaan* is a biometric digital service for pensioners that enables them to generate digital life certificates (DLCs) through *Aadhaar*-based authentication. This service allows more than 10 million families that rely on pensions to use smartphone cameras for DLC generation.

The *Jeevan Pramaan* mobile application is particularly beneficial for elderly pensioners who find it difficult to be physically present at designated centres. The overall processing time for DLC generation has been significantly reduced from 20 days to less than three days through this app. This time-saving measure not only eases the burden on pensioners but also streamlines the administrative process.

*Jeevan Pramaan* has achieved remarkable success since the face authentication campaign in November 2023. It has generated more than 12 million certificates. This enhancement has further simplified the verification process, which ensures a secure and efficient system for pensioners nationwide.



## **2.2. Integration and deployment of face authentication as an AUA**

This section provides a detailed guide for entities that seek to incorporate face authentication into their workflow and customer-facing applications. It details the specifications, considerations, and suggested workflows to integrate, test, and deploy face authentication. If you are not an AUA or KUA yet and are interested to become one, please visit the [UIDAI website](#)<sup>20</sup> and follow the official process to become an AUA or KUA and start using the UIDAI authentication.

Pre-requisites to onboarding and integrating face: Entities need to submit an information system audit of the mobile application essentially covering a Vulnerability Assessment and Penetration Testing (VAPT) and source of the mobile application audited by a CERT-in auditor.

### **2.2.1. Technical specifications of the registered devices for biometric authentication**

The UIDAI ensures the reliability and integrity of the authentication process by using standardised formats and stringent security measures that AUAs and KUAs need to follow. While device registration is not required for face authentication, the device must be capable of downloading and running the FaceRD application developed by the UIDAI, which is available both on the Google Play Store and IOS App Store.

The key components required to perform face authentication are shown below:

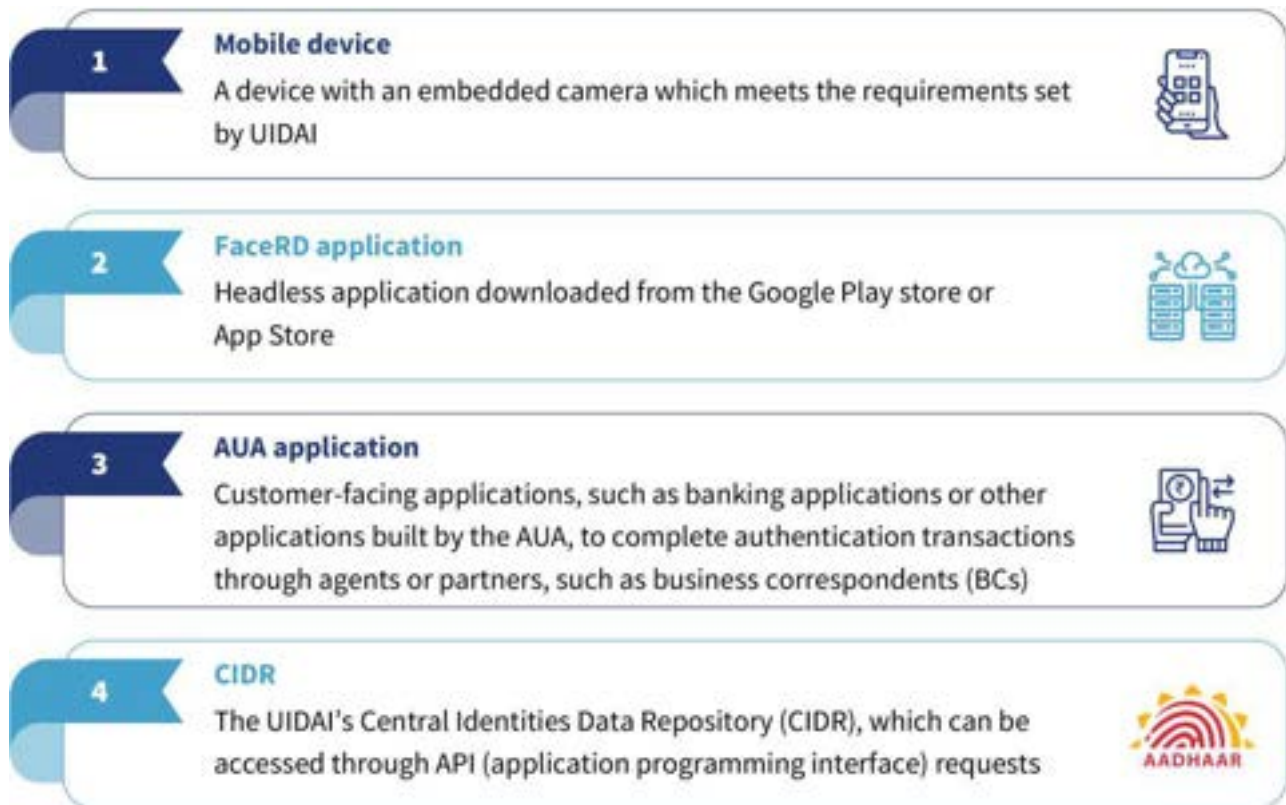
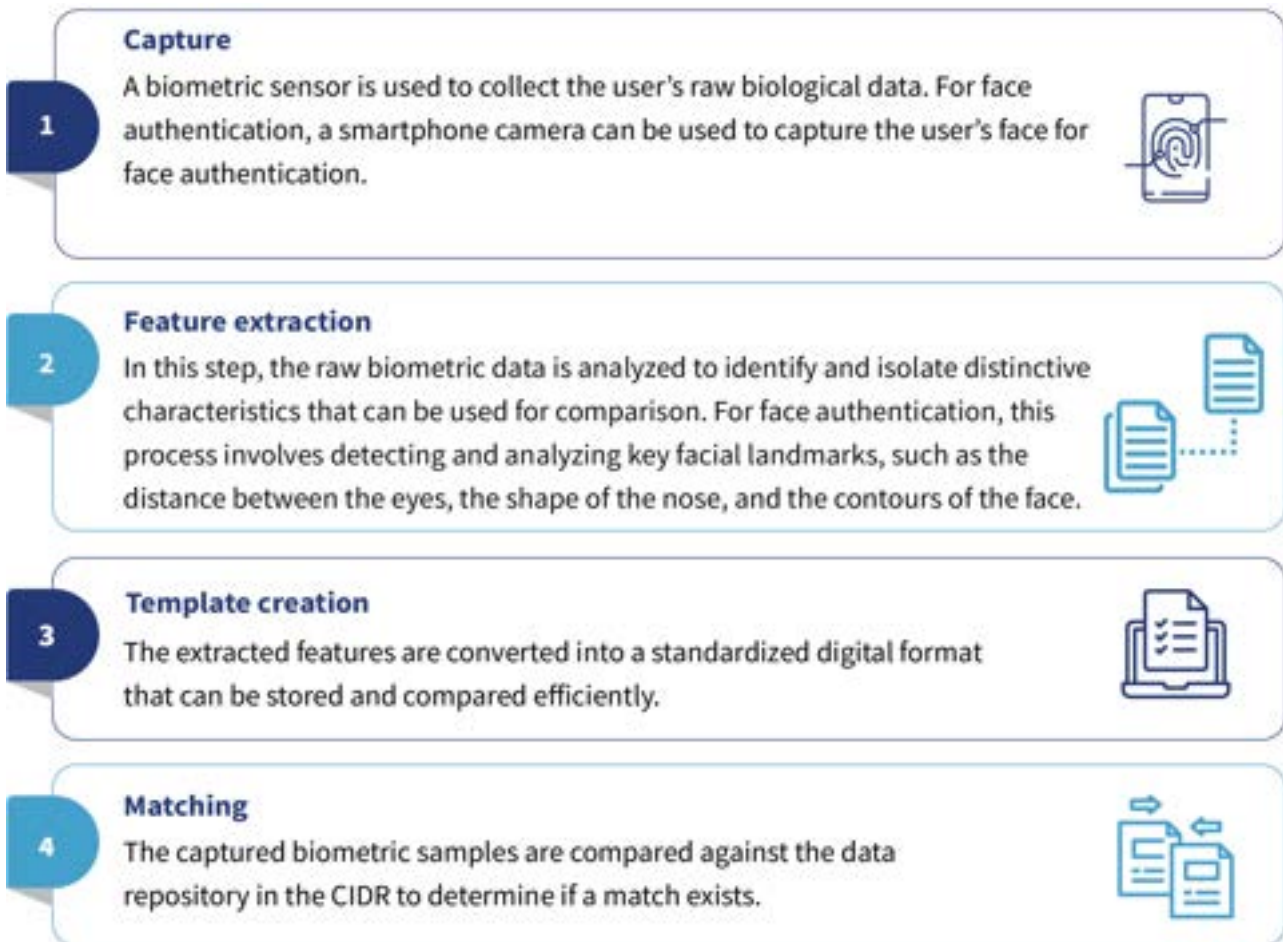


Figure 10: Pre-requisites for face authentication





The biometric authentication process involves certain key steps that all AUAs and KUAs need to follow. While conducting face authentication, the device completes step 1, while the FaceRD application completes steps 2 and 3 and sends the extracted features in a template to the AUA application that can be shared for matching in step 4.



### 2.2.2. Requirements and considerations to integrate face authentication

Any entity that wishes to integrate face authentication into its services should follow the multi-step guidelines listed in the sections below. This guide will walk you through the journey of successfully implementing face authentication. Successful integration of face authentication requires the concerned AUAs or KUAs to fulfil some specifications:

- **Hardware compatibility:** The FaceRD application requires a suitable Android smartphone based on the criteria listed below.
- The UIDAI has provided guidelines on device specifications for both Android and IOS (**M** represents that the specification is mandatory)

Feature	Android	iOS
Android/iOS API version	Android 9 (SDK 28) or greater – M	iOS 14 or greater – M
Disabled USB ports	Yes – M	Yes – M
Non-rooted OS (Google Play Store Compatible)	Yes – M	Yes – M
RAM	4+ GB	4+ GB
Disk space	64 GB (Minimum 500 MB free disk space)	64 GB (Minimum 500 MB free disk space)
Display size (For assisted modes)	5.5" +	5" +
Connectivity	Wi-Fi and GSM	Wi-Fi and GSM
Camera resolution	13 MP +	12 MP +
Camera types	Integrated rear and front camera	Integrated rear and front camera

- **User consent management:** The AUAs have to ensure one of the following practices to inform users and collect consent to conduct the authentication, irrespective of the mode of the authentication transaction – whether self-use or assisted. They also need to ensure that systems preserve the evidence of consent:
  - **SMS with the notice and OTP:** SMS with notice and OTP is sent to the users' phones for validation.
  - **Verbal notice from operators:** The operator will follow a pre-defined script to give verbal notice to the user.
  - **Automated voice recording from the device:** The application has the functionality to read out the notice text to the user in their preferred language.
  - **Check box notice:** The notice text is also a part of the application source code.

### 2.2.3. Integration using API calls

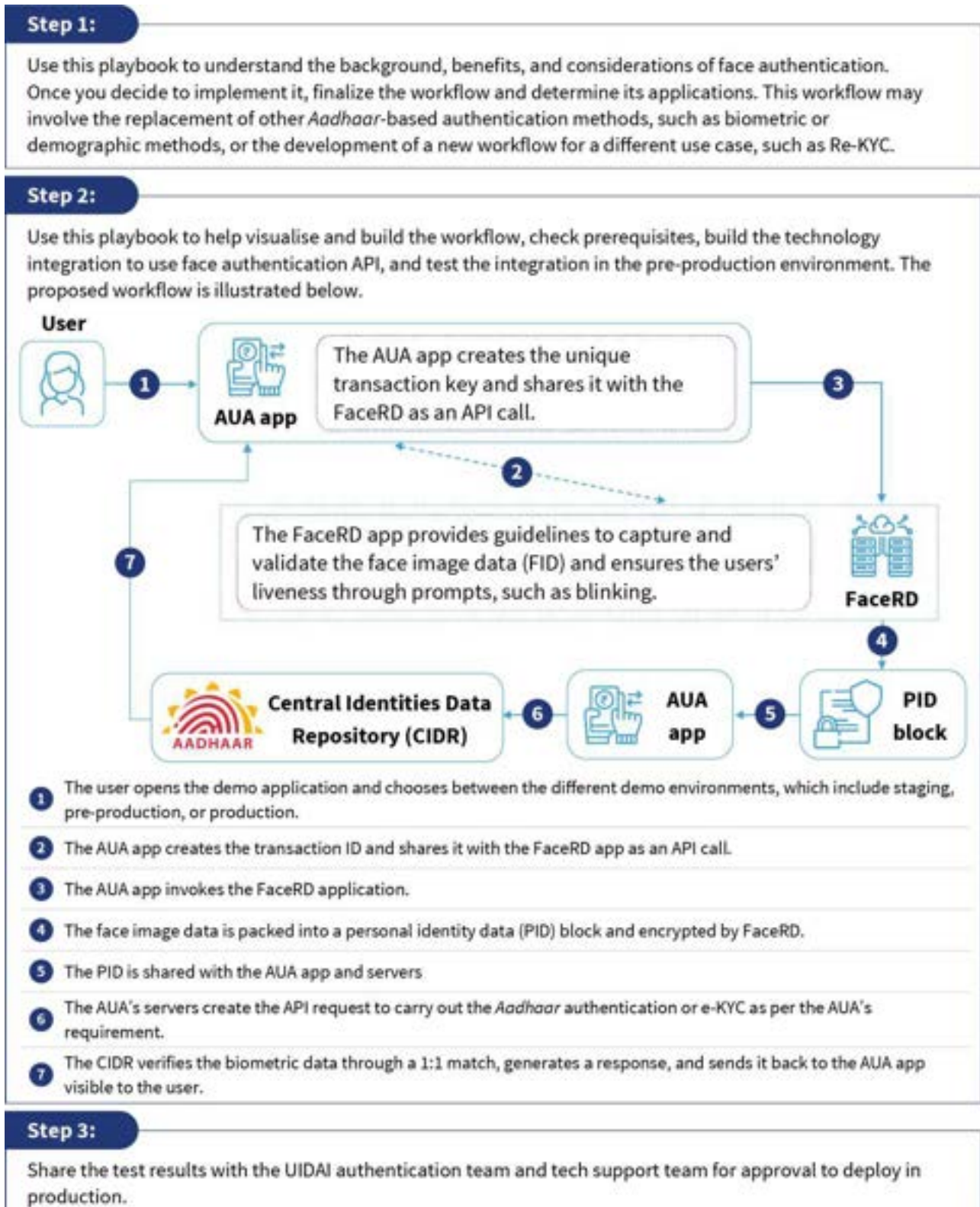
Once the entity's AUA status is established and the infrastructure to orchestrate AUTH call is in place, the AUA should focus on understanding the basics of the *Aadhaar* FaceRD application. The FaceRD application provides a secure interface to capture a live image for *Aadhaar* authentication or eKYC as required.

The API calls in the FaceRD application define the structure of requests and responses and ensure consistent and predictable interactions between the AUA application and FaceRD. Please refer to the API specification document [here](#)<sup>21</sup>. For more information and support, you can contact the authentication support team at UIDAI ([authsupport@uidai.net.in](mailto:authsupport@uidai.net.in)).

## 2.2.4. Demo workflow for face authentication

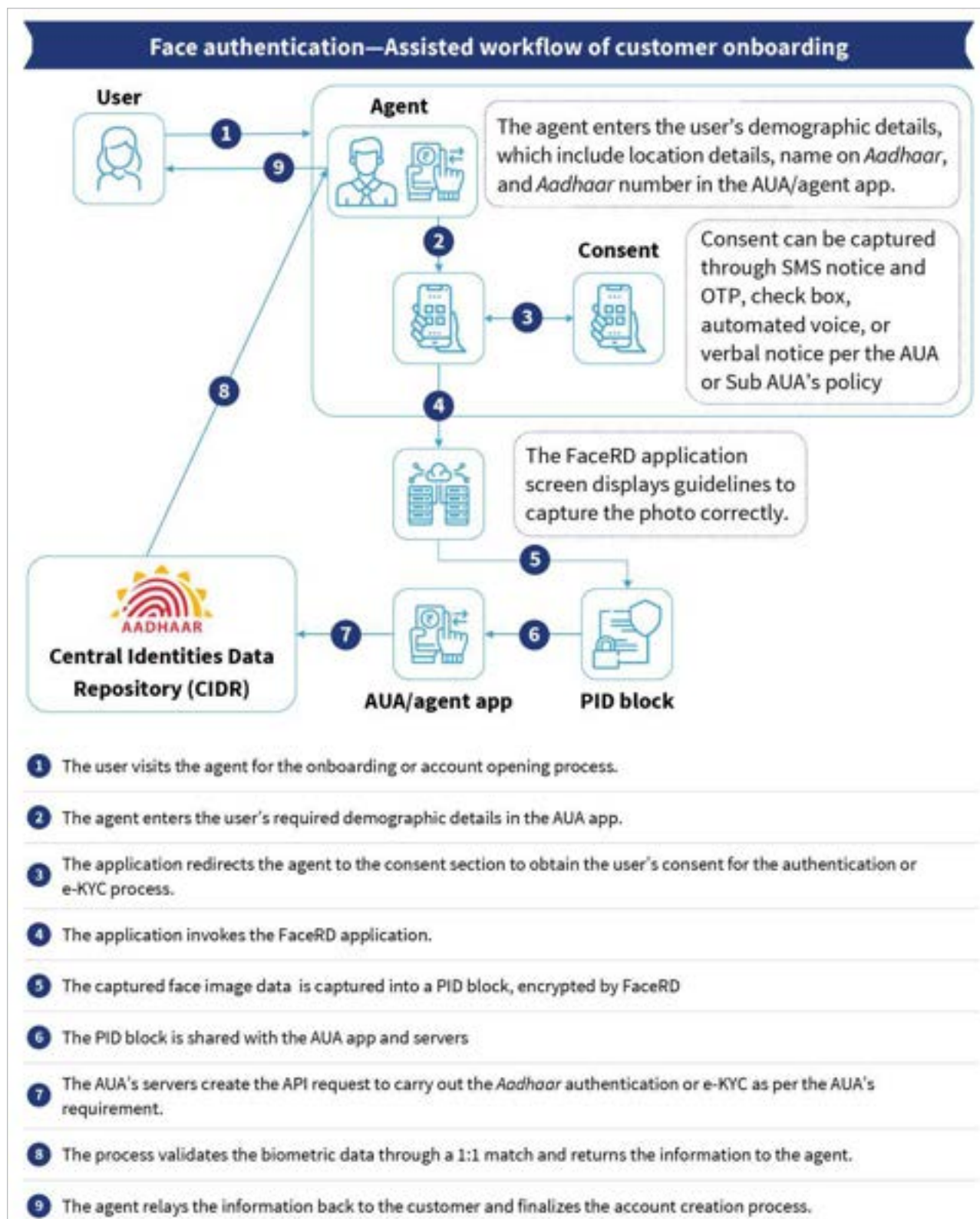
### a) Demo workflow for testing in pre-production

Before an AUA deploys face authentication, they need to complete a pre-production phase for overall testing of the face authentication mechanism. This phase will check the overall integration, validate the transaction flow, and identify potential error codes or security lapses. The illustrative workflow below shows a high-level flow of the pre-production process for an existing AUA or Sub-AUA.



## b) Demo workflow for assisted transactions through face authentication

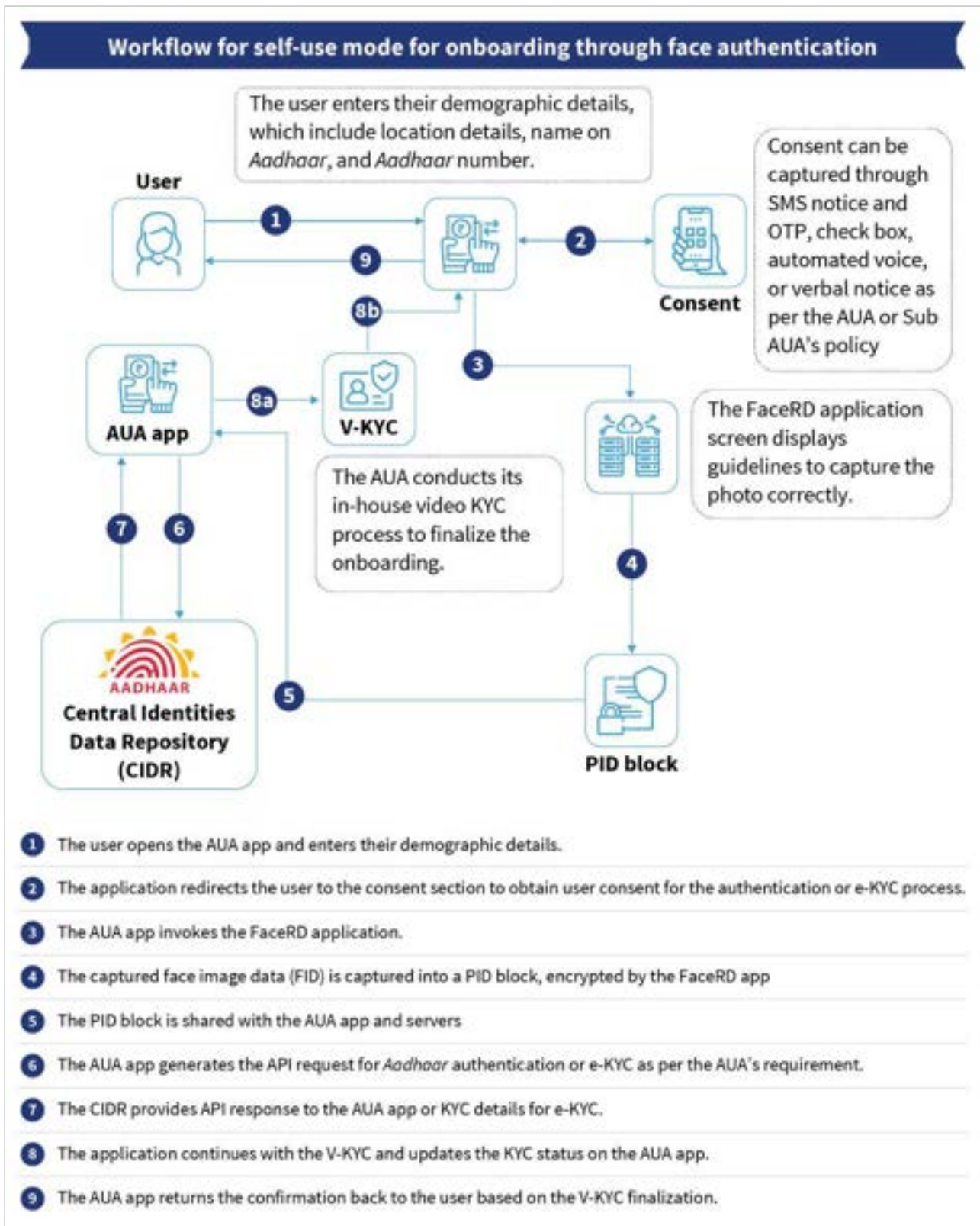
Once the AUA completes the pre-production testing process for face authentication, they can then integrate face authentication as a modality into their workflow. Presently, customer or beneficiary onboarding through assisted modes is a key use case for face authentication. Many entities, such as telecom players, banks, and central and state government programmes, have increasingly used face authentication for their onboarding processes. You can refer to the illustrative workflow below to understand what the real-world application of face authentication would look like.





### c) Workflow for self-service onboarding through face authentication

Presently, the AUAs undertake customer onboarding through face authentication. Once this succeeds, the complete KYC is done through a video KYC. Several banks are currently in the PoC and testing phase of implementing this workflow. An illustrative workflow to implement face authentication within the video KYC flow is shown below:



# 3

## Way forward for face authentication



Face authentication, being an AI/ML-based headless application, is poised to revolutionise the authentication ecosystem in India, with immense potential for expansion across various sectors. Validation and scaling-up of the existing use cases could transform customer experiences as they would provide seamless, frictionless transactions across a broader range of financial and non-financial use cases. As more industries adopt this technology, customers will benefit from reduced fraud and risks, quicker transactions, and a more personalised and efficient service experience.

The growing usage of *Aadhaar* and the evolving financial and technological landscape highlights the ample potential of *Aadhaar*-based authentication across several new use cases.

## 3.1. Potential use cases of face authentication

India has been a leading player in the digital identity ecosystem globally due to *Aadhaar*'s successful adoption and use across different sectors, such as government initiatives, payments, banking and finance, and education, among others. With the introduction of face authentication, we see several potential use cases in different industries.

### Financial use cases:

#### Banking and BCs:

**Fully digital account opening:** Face authentication can also be used to open a fully digital bank account in the self-assisted mode. Customers can open accounts remotely by verifying their identity through face authentication. This eliminates the need for physical presence and paperwork, streamlines the onboarding process, and enhances customer convenience. Given the potential convenience factors, several banks have indicated a potential to onboard more than 200,000 to 300,000 customers monthly. For instance, sharing of the SDKs or the library can enable the AUAs to create independent applications or web interfaces with embedded face authentication modality, which would then reduce the overall download requirement to conduct authentication transactions. Such sharing of the SDKs or the library can be used even to verify the customers for any reason.

#### Payments:

**Enhancement of fraud management:** Face authentication can serve as a powerful tool for fraud management in financial services. It can be used for high-value financial transactions to ensure a high level of assurance. AI and ML models can integrate face authentication with other biometric factors, such as voice or fingerprint, to create multi-factor authentication systems. This layered approach enhances security and reduces the chances of fraudulent access.

AI and ML models can detect potentially fraudulent transactions or account access by detecting anomalies, fake facial features, or synthetic images generated by attackers, and the system can automatically block the account. If users need to unblock the account or proceed with a flagged transaction, they must verify their identity using face authentication. For instance, [Vietnam](#)<sup>22</sup> has integrated facial recognition technology for large bank transfers to ensure safety and reduce the overall risk of fraud.



## Good governance use cases:

**Good governance and access to government services:** People can use face authentication to access e-governance portals to enhance security and improve user experience. The government web portals or mobile applications can integrate *Aadhaar* authentication to provide users with an alternate way to sign in. These applications can utilise the self-service face authentication workflow for signing in. The use of face authentication for sign-in could provide users with an easier way to verify their identity and eliminate the extra steps taken to log in. Additionally, other DBT programs, scholarships, and livelihood programs can start using face authentication to ease the process of disbursement of benefits.

## Other applications of face authentication:

- Besides sectorial use cases for authentication and eKYC, face authentication can be used for other use cases, such as single sign-on across sectors, such as banking and e-commerce, for users to log in to their accounts.
- Face authentication can also be used while designing other processes, such as risk-based authentication systems. Risk-based authentication, a type of adaptive authentication, first assesses the risk of an authentication request initiated by a user and accordingly adapts their authentication mechanisms. Due to its high security and accuracy, face authentication can be used as the primary authentication factor with or without an additional factor to authenticate high-risk transactions, while traditional biometrics, such as fingerprints, can be used for low-risk transactions.





## 3.2. The UIDAI's efforts to enhance the adoption of face authentication

AUAs and sub-AUAs must consider several risks and challenges when they implement face authentication. Cyber fraud and deepfakes pose significant security challenges for financial transactions using face authentication. However, the UIDAI's process uses a match score based on an analysis of facial contours and measurements of the distances between landmarks, such as the eyes and the nose to the mouth. This proprietary algorithm enhances the security of financial transactions.

While the UIDAI's current algorithm addresses current threats effectively, UIDAI continually refines its fraud detection mechanisms to provide even higher security levels. Users might also worry about spoofing the face authentication algorithm with photographs. To counter this, the UIDAI has integrated liveness detection algorithms that prompt users to perform small actions, such as blinking or smiling, to confirm their presence. These algorithms significantly reduce the possibility of photo spoofing. The UIDAI continuously enhances this security feature by adding varied prompts to ensure the check remains unpredictable.

The UIDAI will continue to incorporate feedback from the stakeholders involved in the authentication ecosystem and address key areas, such as security, accessibility, and integration, through continued collaboration with industry stakeholders.

Face authentication holds immense potential to transform the delivery of financial and non-financial services in India. With this technology, institutions can significantly enhance security, streamline customer interactions, and make services more accessible, especially to underserved and remote populations. As this technology continues to evolve, its widespread adoption could positively impact India's digital landscape and make essential services more accessible to all segments of the population.

However, the successful integration of face authentication hinges on the collaborative efforts of the entire ecosystem, which includes policymakers, technology providers, financial institutions, and consumers. Stakeholders can unlock the full potential of face authentication by working together to address the concerns surrounding this modality, drive broader adoption, and contribute to improved financial inclusion across the nation.

## 4. Abbreviations

<b>AI/ML</b>	Artificial Intelligence/Machine Learning
<b>API</b>	Application Programming Interface
<b>ATM</b>	Automated Teller Machine
<b>AUA</b>	Authentication User Agency
<b>AeBAS</b>	<i>Aadhaar</i> -Enabled Biometric Attendance System
<b>AePS</b>	<i>Aadhaar</i> -Enabled Payment System
<b>BC</b>	Business Correspondent
<b>CBC</b>	Corporate Business Correspondent
<b>CERT-in</b>	Indian Computer Emergency Response Team
<b>CIDR</b>	Central Identities Data Repository
<b>COVID-19</b>	Coronavirus Disease 2019
<b>DBT</b>	Direct Benefit Transfer
<b>DLC</b>	Digital Life Certificate
<b>DoT</b>	Department of Telecommunications
<b>FID</b>	Finger Image Data
<b>FIR</b>	Fingerprint Image Record
<b>FMR</b>	Fingerprint Minutia Record
<b>FaceRD</b>	Face Registered Device
<b>GPS</b>	Global Positioning System
<b>IPPB</b>	India Post Payments Bank
<b>KUA</b>	e-KYC User Agency
<b>KYC</b>	Know Your Customer
<b>NIC</b>	National Informatics Centre

<b>OS</b>	Operating System
<b>OTP</b>	One-Time Password
<b>PAHAL</b>	<i>Pratyaksh Hastantrit Labh</i> scheme
<b>PDS</b>	Public Distribution System
<b>PID</b>	Personal Identity Data
<b>PM-FBY</b>	<i>Pradhan Mantri Fasal Bima Yojana</i>
<b>PM-JAY</b>	<i>Pradhan Mantri Jan Arogya Yojana</i>
<b>PM-KISAN</b>	Pradhan Mantri Kisan Samman Nidhi
<b>PMUY</b>	Pradhan Mantri Ujjwala Yojana
<b>PoC</b>	Proof of Concept
<b>PreProd</b>	Pre-Production
<b>Prod</b>	Production
<b>RBI</b>	Reserve Bank of India
<b>SDK</b>	Software Development Kit
<b>STQC</b>	Standardisation Testing and Quality Certification
<b>Sub-AUA</b>	Sub-Authentication User Agency
<b>TAT</b>	Turnaround Time
<b>UIDAI</b>	Unique Identification Authority of India
<b>UPI</b>	Unified Payments Interface
<b>UT</b>	Union Territory
<b>VAPT</b>	Vulnerability Assessment and Penetration Testing
<b>e-KYC</b>	Electronic Know Your Customer
<b>iOS</b>	iPhone Operating System

# Endnotes

<sup>1</sup> [https://uidai.gov.in/aadhaar\\_dashboard/](https://uidai.gov.in/aadhaar_dashboard/)

<sup>2</sup> <https://dbtbharat.gov.in/>

<sup>3</sup> UIDAI data as on as on 15th August 2024 ([https://uidai.gov.in/aadhaar\\_dashboard/ekyc\\_trend.php](https://uidai.gov.in/aadhaar_dashboard/ekyc_trend.php))

<sup>4</sup> Source: UIDAI data

<sup>5</sup> <https://www.thehindu.com/news/cities/Tiruchirapalli/pilot-project-on-iris-based-authentication-in-ration-shops-begins-in-tiruchi/article67610788.ece>

<sup>6</sup> Source: UIDAI data

<sup>7</sup> While the success rate of face authentication transactions remains fairly high, they typically fail due to biometric mismatch errors. This error occurs when the residents fail to update their face image from the time since the original image was captured during their *Aadhaar* enrolment. Transactions have a change of failure for people with significant changes to their facial features in the past 10+ years. Such people are advised to update their biometrics at the earliest to avoid further transaction failures.

<sup>8</sup> <https://www.thehindu.com/news/national/aadhaar-enabled-payment-comprised-11-of-financial-frauds-i4c-analysis/article67706780.ece>

<sup>9</sup> [https://www.business-standard.com/india-news/around-1-1-million-financial-fraud-cases-registered-in-2023-shows-data-124020601528\\_1.html](https://www.business-standard.com/india-news/around-1-1-million-financial-fraud-cases-registered-in-2023-shows-data-124020601528_1.html)

<sup>10</sup> <https://www.medianama.com/2024/07/223-aadhaar-breaches-in-land-records-behind-aeps-fraud-surge/>

<sup>11</sup> Source: NPCI data

<sup>12</sup> Source: NIC data

<sup>13</sup> <https://abdm.gov.in/>

<sup>14</sup> <https://services.india.gov.in/service/detail/jagananna-videshi-vidya-deevena-scheme-andhra-pradesh>

<sup>15</sup> <https://civilsupplies.telangana.gov.in/>

<sup>16</sup> <https://www.bharatpetroleum.in/our-businesses/Bharatgas/Domestic.aspx>

<sup>17</sup> <https://pmuy.gov.in/>

<sup>18</sup> <https://mopng.gov.in/en/marketing/pahal>

<sup>19</sup> Source: NIC data

<sup>20</sup> <https://uidai.gov.in/en/ecosystem/authentication-ecosystem/authentication-requesting-agency.html>

<sup>21</sup> [https://uidai.gov.in/images/resource/Aadhaar\\_Authentication\\_API-2.5\\_Revision-1\\_of\\_January\\_2022.pdf](https://uidai.gov.in/images/resource/Aadhaar_Authentication_API-2.5_Revision-1_of_January_2022.pdf)

<sup>22</sup> <https://asia.nikkei.com/Business/Technology/Vietnam-requires-facial-recognition-for-digital-payments>



If you are interested and ready to engage with the UIDAI team after reviewing the playbook, we can support you in several ways:



## Incubation model



- The UIDAI's tech division in Bengaluru offers regular check-in calls with AUAs and KUAs to assist during pilots and integration phases. For support, you can reach out to our authentication support team at [authsupport@uidai.net.in](mailto:authsupport@uidai.net.in)

## Innovation sandbox



- The UIDAI has launched an Innovation Sandbox that serves as an innovation-oriented portal where you can test current and upcoming UIDAI services. It will be a platform where innovators and researchers can develop applications and tools.
- You can use the sandbox to check out and test features, such as digital onboarding, integration with API services, and federated login using *Aadhaar* and more—without requiring direct access to the production environment or datasets.
- We invite stakeholders across sectors that utilise UIDAI services, tech innovators, academia, and research groups to collaborate with us through this sandbox and other engagement mechanisms, including cohorts, competitions, and hackathons. The features and capabilities of the sandbox will be rolled out in phases—stay tuned for more details on how you can get involved!

“ When I discover who I am, I’ll be free ”

- Ralph Ellison, Invisible Man







**Unique Identification Authority of India**  
Government of India



## UIDAI Head Office

Government of India Bangla Sahib Rd, Behind Kali Mandir, Gole Market, New Delhi - 110001

For more information, please contact us at [help@uidai.gov.in](mailto:help@uidai.gov.in)

Follow us on:    

Copyright © 2022 Unique Identification Authority of India All Rights Reserved

Knowledge Partner

